AF/ ~~2131~~

cc
2700

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of **Michael A. Epstein**	Atty. Docket No.: **PHA 23-313**
Serial No.: **08/994,878**	Group Art Unit: **2131**
Filed: **12/19/97**	Examiner: **Ho S. Song**

Title: **ADMINISTRATION AND UTILIZATION OF PRIVATE KEYS IN A NETWORKED ENVIRONMENT**

Honorable Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

Enclosed is an original plus two copies of an Appeal Brief in the above-identified application.

[X] A credit card authorization in the amount of **$320** is enclosed.

[ ]The Commissioner has already been authorized to charge fees in this application to Deposit Account .

[ ]The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account _________. Enclosed is a copy of this sheet.

Respectfully submitted,

Robert M. McDermott, Esq.
Reg. No. 41,508
804-493-0707

CERTIFICATE OF MAILING

It is hereby certified that this correspondence is being deposited with the United States Postal Service as first-class mail in an envelope addressed to: COMMISSIONER OF PATENTS AND TRADEMARKS, Washington, D.C. 20231

On 4 February 2003 By ____________.

#27

1 of 3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of **Michael A. Epstein**	Atty. Docket No.: **PHA 23-313**
Serial No.: **08/994,878**	Group Art Unit: **2131**
Filed: **19-Dec-1997**	Examiner: **Hosuk Song**

Title: **ADMINISTRATION AND UTILIZATION OF PRIVATE KEYS IN A NETWORKED ENVIRONMENT**

APPELLANT'S BRIEF ON APPEAL UNDER 37 C.F.R. § 1.192

Honorable Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

This is an appeal from the decision of the Examiner dated 26 September 2002, finally rejecting claims 5-8 of the subject application.

I. REAL PARTY IN INTEREST

The above-identified application is assigned, in its entirety, to Philips Electronics North America Corporation, a company organized under the laws of the State of Delaware.

II. RELATED APPEALS AND INTERFERENCES

Appellant is not aware of any co-pending appeal or interference which will directly affect or be directly affected by or have any bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 5-8 are pending in the application. Claims 5-8 stand rejected by the Examiner under 35 U.S.C. 103(a) as being unpatentable by Trostle (USP 5,919,257) in view of Asay et al. (USP 5,903,882, hereinafter Asay).

IV. STATUS OF AMENDMENTS

An amendment was filed subsequent to the final rejection in the Office Action dated 26 September 2002, but the Examiner has determined that the proposed amendment did not place the application in better form for appeal.

V. SUMMARY OF THE INVENTION

The invention comprises a method for the administration and control of private keys of users within a network of communicating devices, or terminals.

Conventionally, each terminal on a network is associated with a particular user. The user, for example, has a personal computer (PC) at his or her workplace that is coupled to the network, and may or may not have a personal digital assistant (PDA) device, or other portable communicating device, that is also coupled to the network.

Private encryption keys are used to encrypt documents, or to digitally sign documents. A public key that corresponds to a user's private key, in a public-private key pair arrangement, is used to decrypt the encrypted documents, or to verify the user's digital signature. Generally, each key is a large, multi-byte, random number. A user is not expected to memorize the large random number corresponding to his or her private key; rather, the private key is stored in a file at each of the user's terminal. To prevent unauthorized access to the user's key, a password protection scheme is commonly used to limit access to the user's terminal, or to limit access to the user's key. Once a user securely logs into a terminal and network, conventional systems generally assume that the terminal is controlled by the user until the user logs out, or until a time limit is expired.

The paradigm of a terminal that is associated with a user, however, becomes inappropriate as networked terminals become ubiquitous. In an office environment, for example, a user may have a PC terminal and a telephone at his or her workspace. In a public area, such as a conference room, cafeteria, laboratory, and so on, the user will commonly place or receive telephone calls using any available telephone instrument in the user's vicinity. In like manner, users in networked systems can be expected to routinely use networked terminals based on their proximity to the user, rather than based on their possession by the user. In this environment, the assumption that the user's private key will be located at the user's terminal no longer holds true, and the assumption that the user is in control of the terminal until the user logs out relies heavily on the conscientiousness of the user to effect a proper log-out.

This invention provides a particularly effective and efficient method for administering and controlling users' private keys in a networked environment, wherein private keys are not retained at users' terminals, but are communicated to the terminal on demand from a server (Applicant's specification, page 3, line 28 through page 4, line 1). In accordance with the principles of this invention, an encrypted form of each user's private key is stored at a server facility (Applicants' specification, page 4, lines 2-8). When the user requires the private key, the user communicates an ID to the server, from any terminal on the network, and the server communicates the encrypted private key to the terminal. The user decrypts the private key at the terminal, based on a highly secure decryption key, or user identifying key, such as biometric information associated with the user, or a multi-word pass phrase (Applicant's specification, page 4, lines 15-25, and page 9, lines 2-18). The decrypted private key is then used to encrypt information, such as a hash of a document, constituting a digital signing of the document (Applicant's specification, page 5, lines 13-26). Upon completion of the encryption, the private key is deleted from the terminal (Applicant's specification, page 13, line 24 through page 14, line 1).

To assure that the user is actually present at the terminal when a given document is submitted for transmission, the server of this invention transmits the user's encrypted private key to the terminal, then validates the document only if the document is digitally signed using the decrypted private key. In combination with a terminal that is configured to delete the user's private key after each use, this process assures the presence of the user at the terminal when the document is signed. Because the decrypted private key is deleted after each use, the technique of this invention is particularly well suited for a network of terminals that are accessible by a variety of users.

VI. ISSUES

Are claims 5-8 patentable under 35 U.S.C. 103(a) over Trostle in view of Asay?

VII. GROUPING OF CLAIMS

Claims 5-8 stand or fall together.

VIII. ARGUMENT

Are claims 5-8 patentable under 35 U.S.C. 103(a) over Trostle in view of Asay?

In claim 5, upon which each of the other rejected claims depends, the Applicant specifically claims destroying, or avoiding making, any non-volatile record of the private key at the location of the user.

Trostle teaches a method and system for detecting whether an executable program at a user terminal, or workstation, has been illicitly changed (Trostle's Abstract). Trostle's process includes the transmission of an encrypted private key from a server to the workstation, and the decryption of the private key at the workstation, based on a user password. The Examiner acknowledges that Trostle does not teach destroying the non-volatile record of the private key at the location of the user.

The Examiner maintains that Asay teaches destroying any non-volatile record of the private key at the location of the user. The Applicant respectfully traverses this characterization of Asay.

Asay specifically teaches the storage of an 'encrypted' copy of the user's key at the location of the user to facilitate subsequent use of the user's key at that location. In Asay, a 'clear' copy of the key is destroyed, but an encrypted copy of the key is made and stored. The Applicant specifically recites in claim 5 that ***any***[1] non-volatile record of the key is ***destroyed*** or ***not made***. Asay specifically teaches ***making, saving, and not destroying*** at least one non-volatile record of the key, to facilitate a reconstruction of the key. The Applicant respectfully maintains that by common definition of the term, "***any***

[1] In the referenced after-final amendment that was not admitted by the Examiner, the Applicant's proposed amendment recited "any and all non-volatile records", to make it clear that the term "any" as used in the claims is inclusive. Because the Examiner has determined that this proposed amendment did not place the claim in better condition for allowance or appeal, it must be assumed that the term "any" is interpreted to be inclusive, and specifically, to include any and all records of the user's key.

non-volatile record" includes the "encrypted non-volatile record" of the user's key that Asay specifically creates, and does not destroy.

The Examiner references a sentence in Asay that directs the "destruction" of a private key (Asay, column 30, lines 55-57). This sentence, however, is prefaced with "the corresponding private key ***is stored in a safe place in the subscriber's system***" (Asay, column 30, lines 53-54).

The Applicant respectfully maintains that Asay ***teaches against*** the Applicant's claimed destruction of any non-volatile record of the user's private key, because Asay specifically teaches ***making a non-volatile record*** of the user's private key, and does ***not*** teach ***destroying*** this non-volatile record of this private key, as specifically claimed by the Applicant.

CONCLUSIONS

Because Asay specifically teaches the saving of a non-volatile version of a user's key at the user's terminal, whereas the Applicant claims the destruction of any non-volatile version of the user's key at the user's terminal, the Applicant respectfully requests that the Examiner's rejection of claims 5-8 under 35 U.S.C. 103(a) over Trostle in view of Asay be reversed by the Board, and the claims be allowed to pass to issue.

Respectfully submitted,

Robert M. McDermott, Attorney
Registration Number 41,508
804-493-0707

APPENDIX

CLAIMS ON APPEAL

5. A method for obtaining and using a private key at user equipment via a network, said method comprising:

transmitting from the user equipment an ID of a user;

receiving a private key of the user encrypted with a user identifying key associated with the user; and

decrypting the encrypted private key using a user identifying key determined from interaction with the user at the user equipment;

using the decrypted private key; and

destroying or avoiding making any non-volatile record of the private key at the location of the user.

6. The method of Claim 5, wherein

the user identifying key determined by interaction with the user at the user equipment is determined from a passphrase entered by the user at the user equipment or biometric information which is obtained from the user by suitable measurement or scanning at the user equipment.

7. A method as claimed in Claim 5, wherein the decrypted private key is used by:

computing a hash of a document to manifest the user's approval of the document;

encrypting the hash using the user's private key; and

transmitting the encrypted hash.

8. A method as claimed in Claim 6, wherein the decrypted private key is used by:

computing a hash of a document to manifest the user's approval of the document;

encrypting the hash using the user's private key; and

transmitting the encrypted hash.